CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement before the Committee on Oversight and Reform Subcommittee on Management, Organization and Procurement

"CYBERSECURITY: EMERGING THREATS, VULNERABILITIES AND CHALLENGES IN SECURING FEDERAL INFORMATION SYSTEMS"

A Statement by

James A. Lewis

Director and Senior Fellow, Technology and Public Policy Program

Center for Strategic and International Studies (CSIS)

May 5, 2009

I thank the Committee for the opportunity to testify.

Digital networks provide real economic benefit. However, the combination of greater reliance on networks and inadequate attention to security has left our nation vulnerable. My written statement lists publicly known incidents in just the last year. The failure to secure America's information infrastructure weakens the United States and makes our competitors stronger.

The risk to the U.S. lies in long-term damage to economic competitiveness and technological leadership. We are everyone's target. Cyber attacks are illicit action to penetrate computer networks. This provides the capability to disrupt key services, as in the case of an opponent who accesses an utility's control system, but the immediate problem involves the theft of intellectual property and advanced commercial and military technology to foreign competitors.

Right now, attackers have the advantage in cyberspace. The principle threat comes from well-financed and innovative opponents. The most skilled are foreign military and intelligence services with immense resources and experience – the first Russian hack of DOD computers occurred more than 25 years ago. These government agencies are almost matched by highly sophisticated cybercriminals who buy and sell tools and data in black markets that are virtual arms bazaars for attackers and who are safe from the threat of prosecution.

The sources of vulnerability are outdated policy and laws and inadequate technologies. The internet as it is currently configured and governed cannot be secured. If we continue on the course we are on today, where we have not learned how to balance the efficiency information technology provides with the need to secure it, these vulnerabilities will grow.

The United States has been trying to improve cybersecurity for more than a decade. The last twelve months have seen some progress and the Obama administration has identified cybersecurity as an important issue for national security. But we still are fundamentally confused.

There are arguments that the government should only secure its own networks and lead by example. This won't work, since we are all really on one big network, government and private sector, American and foreigners. It's like saying tune up half the car, and hope the other spark plugs are inspired. A partial solution will fail. Some say that since most networks are privately owned, we should rely on the private sector for defense. This is like saying that since most airplanes are private, we should depend on the airlines to defend our airspace. National security is a function that only the government can perform adequately. People worry that if we secure our networks, it will damage America's ability to innovate. But more investment in innovation is pointless if we are only going to share it for free with our foreign competitors.

We need a comprehensive, government-led approach to secure cyberspace. In recognition of this, the CSIS Cybersecurity Commission recommended a broad national approach to cyber security, the creation of a strong White House cyber advisor with clear authorities, and development of a national security strategy that would use all the tools of U.S. power.

Government policy will determine whether we fail or succeed. Government acquisition rules can be changed to create a market for more secure products and services. A revised FISMA would improve agency security and provide a template for private sector efforts. International engagement, expanded federal law enforcement, a judicious use of regulatory powers, and investment in education and research can change situation from one where we are losing to one were we are at least holding our own.

The problems we face in cyberspace – espionage, crime and risk to critical infrastructure – will never go away, but the risk they pose can be reduced by coordinated government action based on a comprehensive strategy and clear leadership and authority.

As you know, the Administration is struggling to conclude its sixty-day cybersecurity review. Ideally, the review will lead to a strong White House cyber advisor with clear authority. Without this, our cybersecurity efforts will always be underpowered. But with so many different interests involved, there is a risk that the Administration will come up with a solution that makes everyone happy. The only people who will benefit from this are foreign intelligence agencies and cybercriminals.

I thank you for the opportunity to testify and will be happy to take your questions.